

CYBER INCIDENT RESPONSE POLICY

POLICY# OTECH-POL2021-007

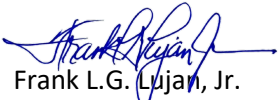
FRANK LG LUJAN JR
OFFICE OF TECHNOLOGY, GOVERNMENT OF GUAM
<https://Otech.guam.gov>



AUGUST 31, 2021



Overview

Policy Number:	OTECH-POL2021-007
Title:	Cyber Incident Response Policy
Purpose:	To provide a process that is required to ensure an organized approach to managing cyber incidents within Government of Guam (GovGuam) entities supported by the Office of Technology (OTECH) and to coordinate response and resolution efforts to prevent or limit damage that may be caused.
Publication Date:	August 31, 2021
Authority:	5 GCA Chapter 1 Article 12.106 (e)
Policy Approval:	 Frank L.G. Lujan, Jr. OTECH, Chief Technology Officer (CTO)
Target Audience:	<p>This Cyber Incident Response Policy is managed by the Office of Technology (OTECH).</p> <p>The intended recipients of this policy includes all entities under the authority of the Office of Technology, pursuant to the provisions of Public Law 34-076.</p>
Contact Details:	Office of Technology 211 Aspinall Avenue Hagåtña, Guam 96910 O: 671.635.4500 F: 671.472.9508 https://otech.guam.gov



Revision History

Date of Change	Responsible	Summary of Change
August 2021	OTech Systems Support	Draft policy
August 2021	CTO, DPM	Review draft, approve and disseminate

Policy Reviews and Updates

Date of Review	Responsible Parties	Summary of Change



Table of Contents

1.0 Introduction	4
1.1 Review	4
2.0 Terminology and Definitions	4
2.1 Cyber Event	4
2.2 Cyber Incident	4
3.0 Common Cyber Incidents and Responses	4
3.1 Potential Threat Vectors	5
4.0 Roles and Responsibilities	5
4.1 OTECH Incident Management Team	5
4.2 OTECH Senior Executive Management Team	6
5.0 Incident Response Process	6
5.1 Detection and Analysis	7
5.1.1 Incident Detection	7
5.1.2 Incident Analysis	7
5.1.3 Incident Classification	8
5.1.4 IMT Activation	9
5.1.5 Incident Notifications	9
5.1.6 IMT Documentation	10
5.2 Containment and Eradication	11
5.2.1 Resolution Action Plan	11
5.2.2 Evidence Preservation	11
5.3 Communication and Engagement	11
5.3.1 Internal Communications	12
5.3.2 External Communications	12
5.4 Recover	12
5.4.1 Stand Down	12
5.5 Learn and Improve	12
5.6 Update Incident Response Policy and Procedures	13
6.0 Compliance	13



1.0 Introduction

Cyber security relates to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, and protecting it and associated systems from external or internal threat. This document supports the Office of Technology (OTECH) in managing contemporary cyber threats and incidents. The application of this document will support OTECH in reducing the scope, impact and severity of cyber incidents.

This document is developed using the National Institution of Standards and Technology (NIST) Computer Security Incident Handling Guide.

1.1 Review

This incident response policy will be reviewed annually by the OTECH Chief Technology Officer (CTO) and the OTECH Incident Management Team (IMT), or following any cyber incident deemed necessary by the OTECH CTO.

2.0 Terminology and Definitions

This section outlines key terminology and definitions used in this plan.

2.1 Cyber Event

A cyber event has the potential to become, but is not confirmed to be, a cyber incident.

Examples of cyber events include (but are not limited to):

- Multiple failed sequential logons for a user
- A user has disabled the antivirus on their computer
- A user has deleted or modified system files
- A user restarted a server
- Unauthorized access to a server or system

2.2 Cyber Incident

A cyber incident occurs when there is a breach of explicit or implicit digital security policy that requires corrective action because it threatens the confidentiality, availability and integrity of an information system or the information the system processes, stores or transmits.

Examples of cyber incidents include (but are not limited to):

- Denial of service attacks (DoS) that affect system or service availability
- Virus or malware outbreak (including ransomware)
- Compromise or disclosure of sensitive or personal information
- Compromise of network credentials or an email account

This plan identifies four categories of cyber incidents which are differentiated by the level of impact they create.

3.0 Common Cyber Incidents and Responses

The following table provides a list of common cyber incident types, along with the corresponding response activities (which form the typical minimum response).



#	Type / Description	Initial response to minimize potential harm
1	Ransomware ; a tool used to encrypt or lock victims' data until a ransom is paid.	Immediately remove the infected device(s) from the network to limit the spread of ransomware. Capture all available logs relevant to the device. Isolate the devices while containment and eradication activities are determined.
2	Malware Infections ; a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.	Immediately remove the infected device(s) from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed and eradication efforts are determined.
3	Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks ; overwhelming an ICT network with traffic that it cannot process, sometimes causing the network to fail.	Request gateway services provider to identify DOS/DDOS nature, attack vector and implement suitable solutions. Liaise with gateway services and network team to apply filters at network edge and / or increase capacity.
4	Phishing and Social Engineering ; deceptive communications designed to elicit users' sensitive information (including network credentials).	Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed. Consult users to confirm what actions they took, and whether any personal/sensitive information was provided in response to a phishing/social engineering attempt. Consider resetting user passwords and monitoring accounts for any unauthorized access.
5	Data breach ; unauthorized access to sensitive or personally identifiable information.	Contain the data loss/spill as soon as possible. Alert privacy, legal and communications/media teams. Investigate the cause of the data loss/spill.

3.1 Potential Threat Vectors

There are multiple vectors through which a cyber incident can arise. Maintaining awareness of these threat vectors will support OTECH in identifying potential 'weak spots' or commonly targeted aspects of GovGuam network and systems. Some of the more common vectors include:

#	Type	Description
1	External/removable media	An attack executed from a USB containing malware.
2	Attrition	A DDoS attack on a critical network or system.
3	Web	The redirection of web traffic to a malicious URL that installs malware on a victim's device.
4	Email	Phishing attacks that attempt to steal information and/or deploy malware to a victim's device.
5	Impersonation usage	For example, a domain that is created to imitate yours in an attempt to deceive victims (typically associated with phishing attacks).
6	Improper usage	Human error resulting in a breach of information security policy; or attack from a malicious insider resulting in a cyber security incident.

4.0 Roles and Responsibilities

The following section details the composition and functions of the OTECH IMT and OTECH Senior Management Team (SEMT).

4.1 OTECH Incident Management Team

The OTECH IMT is responsible for managing responses to cyber incidents. Their roles include:

- Incident planning and operations
- Intelligence and analysis



- Technical advice
- Incident investigation
- Facilities support
- Business and community consequence analysis/management
- Information and warnings
- Internal communications
- Administration support including incident log, evidence and situation reporting
- System/application support

4.2 OTECH Senior Executive Management Team

The SEMT should provide strategic oversight, direction and support to the IMT, with a focus on:

- Strategic issues identification and management
- Stakeholder engagement and communications (including ministerial liaison, if appropriate)
- Resource and capability demand (including urgent logistics or finance requirements, and human resources and considerations during response effort).

The OTECH CTO assumes the lead for the SEMT and appoints members for the IMT.

5.0 Incident Response Process

Quick Reference Checklist of Incident Response Actions

#	Activity
1	Conduct analysis to determine whether an incident has occurred / or is occurring
2	Determine the scope, impact and severity of the incident; categorize the incident
3	Activate your IMT and SEMT to manage the response effort; begin documenting the situation
4	Develop and implement a resolution action plan detailing containment, eradication and recovery activities; gather and record evidence
5	Identify affected stakeholders – who will be impacted by the incident?
6	Develop a notifications strategy and communicate key messages with affected stakeholders
7	Confirm the threat has been eradicated and return affected systems/services to normal function (test systems/services to confirm expected functionality)
8	Stand down your IMT/SEMT (when authorized by appropriate delegate); determine any stakeholder communications requirements
9	Conduct a post incident review to identify things that worked well and any opportunities for improvement; document your learnings/insights
10	Update your incident response plan to include any key learnings/insights



5.1 Detection and Analysis

5.1.1 Incident Detection

There is no single process for detecting a cyber incident. Detection often involves:

- **Precursors:** detecting that a cyber-attack might occur in the future, such as the receipt of a threatening email or news of a global malware/ransomware attack (note: this form of detection is rare).
- **Indicators:** detection that an incident may have occurred (e.g. intrusion detection alarms, file names with odd characters, configuration changes).
- **Security Monitoring:** Referral from a managed security service provider or another organization/stakeholder, alerting to the presence of a cyber incident.

The table below provides some common indicators that suggest one might experience a cyber security incident:

Indicators	Examples
Reports of unusual or suspicious activity by staff or external stakeholders.	A staff member receives an email asking them to confirm their network credentials or to provide other personal or sensitive information.
	Multiple staff report being 'locked out' of their network accounts.
	An external stakeholder reports receiving spam or phishing emails from your organization.
	A member of the public approaches your organization to report the discovery (or exploitation) of a security vulnerability.
System(s)/service(s) not operating or functioning as expected	For example, one or more IT systems or services may cease functioning, or may not function as expected, and there is not a readily identifiable cause (such as a planned upgrade or outage).
	SSL Certificates broken; for example customers complaining that your organization's website has a broken link.
Unusual Activity	Network administrators observe a large number of 'bounced' emails containing suspicious or unexpected content; or there is a substantial change in network traffic flows with no readily identifiable cause.
	Network or application logs show multiple failed login attempts from unfamiliar remote systems, such as overseas locations.
	Anti-virus alerts – a notification from your anti-virus service or a managed service provider that it has detected suspicious activity or files on your network, which require analysis and remediation.
	Service or admin accounts modifying permissions; admin accounts adding standard users to groups; service accounts logging into a workstation.
	A system administrator observes a filename with unusual characters, or expected files are no longer visible on the network.

5.1.2 Incident Analysis

After considering the indicators of a potential cyber incident, it is important to confirm whether an incident has, or continues, to occur. The following table identifies steps that are useful in confirming the presence of a cyber incident.

Action	Description
Updated Resources	Ensure you have access to the latest:



Action	Description
	<ul style="list-style-type: none">- Network diagrams- IP addressing schemas- Port lists- Documentation that may include system designs/architecture, security plans, GPO configuration, etc.
Reviewing log entries and security alerts	Are there any unusual entries or signs of suspicious behavior on the network or applications?
Have Standard Operating Procedures (SOPs) for different operating systems	For Windows workstations, follow a SOP on what to look for or review (i.e. specific event log sources, the types of events to search for, etc.). The same applies for Linux and Unix Operating Systems.
Consult with network and application experts	Is there a legitimate explanation for the unusual or suspicious activity that has been observed?
Conduct research	Research and review any open source materials (including via internet search engines) relating to the unusual or suspicious activity that is observed (for example, consider performing a search on any unusual filenames that are observed on the network).
Watch list / monitor list	Develop a list where suspected accounts or IPs can be added to monitor their ongoing activity.
IMPORTANT	Do not 'ping' or try to communicate with a suspected IP address or URL from your own network, as you may tip off the attacker that you have detected their activity. This should be conducted by a third party that is able to conduct this activity securely and anonymously.

Generally, OTECH will dedicate up to one hour on the initial incident analysis phase before seeking outside assistance.

5.1.3 Incident Classification

The following table provides a guide for classifying the category of a cyber incident. The table also provides indicators to consider when determining whether a cyber incident is increasing or decreasing in impact and severity.

Category	Description	Trigger(s) for escalation
Cyber Event	A suspected (or unconfirmed) cyber incident, with no observable impact to systems or services.	Substantial increase in cyber security alerts; or continued cyber security alerts with potential to breach security controls. Confirmed breach of security controls.



Category	Description	Trigger(s) for escalation
Cyber Incident	Successful compromise of security controls that requires corrective action. Minor to moderate impact to services, information, assets, reputation or relationships. May form part of a national or international cyber incident.	Actual or high likelihood: <ul style="list-style-type: none">• for major impact to services; or• to affect multiple organizations; or• data breach involving personal information such as Personally Identifiable Information (PII), Social Security Administration (SSA) provide data, Personal Health Information (PHI) or Federal Tax Information (FTI).
Significant Cyber Incident	Successful compromise of security controls that requires corrective action. Major to significant impact to services, information, assets, government reputation, relationships and/or the community (but not an emergency situation). Any incident that involves: <ul style="list-style-type: none">• more than one organization; or• a data breach involving personal information such as Personally Identifiable Information (PII), Social Security Administration (SSA) provide data, Personal Health Information (PHI) or Federal Tax Information (FTI).	A situation that: <ul style="list-style-type: none">• has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment, or• Has the potential to have or is having significant adverse consequences for the Government of Guam.
Cyber Emergency	Successful compromise of security controls that: <ul style="list-style-type: none">• has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment; or• has the potential to have or is having significant adverse consequences for the Government of Guam; or• requires the involvement of two or more agencies to respond to the emergency.	

5.1.4 IMT Activation

If a cyber incident is confirmed and requires a team to manage the response effort, activate the IMT and SEMT (note: some smaller incidents may be manageable without activation of the IMT).

5.1.5 Incident Notifications

It is important to notify relevant stakeholders that a cyber incident has occurred or is occurring.



The scope, impact and severity of the incident should determine the extent of stakeholder notifications. More serious incidents will likely require engagement with a broader range of stakeholders. The OTECH CTO will determine the list of relevant stakeholders for each cyber incident.

Cyber incidents involving protected data such as Personally Identifiable Information (PII), Personal Health Information (PHI), Social Security Administration (SSA) provided data and Federal Tax Information (FTI) engages a specific notification process. In the event of such a significant cyber incident, OTECH will work directly with the affected Agency's Security Officer and activate the Agency's Incident Response Plan.

OTECH's responsibility to protect SSA-provided data also elevates a higher level of notifications. Cyber incidents involving suspected or the actual loss of Social Security Administration (SSA)-provided information are processed according to the following steps:

1. SO notifies the SSA Regional Office or the SSA Systems Security Contact as identified in the SSA Information Exchange Agreement (IEA) within one hour of notification of the suspected or actual loss of SSA-provided information.
2. If SO is unable to make contact with the SSA Regional Office or the SSA Systems Security Contact within one hour, SO reports the security incident to the SSA's National Network Service Center (NNSC) toll free 877-697-4889 (select "Security and PII Reporting" from the options list). As the final option, in the event SSA contacts and NNSC both cannot be reached, the SO is to contact SSA's Office of Information Security, Security Operations Center at 1-866-718-6425.
3. SO provides updates as they become available to the SSA contact as appropriate.
4. SSA makes a determination about whether the risk presented by the breach or security incident requires the notification of the individuals whose information is involved and remediation action.

5.1.6 IMT Documentation

Upon establishment, the IMT should immediately begin documenting information about the incident. This document includes 'Situation Updates' and the 'Incident Log'.

Situation Updates should contain the following information:

- Incident date and time (usually the date and time the incident was confirmed)
- The status of the incident – for example, new / in progress / resolved
- Incident type and classification – for example, malware / ransomware / DDoS etc.
- Scope – details of affected networks, systems and/or applications
- Impact – details of entities affected by the incident, and how they are affected
- Severity – details of the impact of the incident on the organization(s) (for example, what business services were impacted?)

Situation updates should be prepared and disseminated to OTECH staff members. It is important for OTECH to be proactive with the development and dissemination of all situation reports, to reduce the need for staff members to approach the SEMT or IMT with various questions about the incident.



The **incident log** should be maintained by a member of the IMT (or a delegate). The incident log should capture details of all critical decisions, operational actions taken and action items. Each entry to the incident log should include date, time and author details.

5.2 Containment and Eradication

5.2.1 Resolution Action Plan

The IMT (or delegate) should develop a **Resolution Action Plan** for resolving the cyber incident.

The Resolution Action Plan should consider the immediate and future steps required for containing the incident and eradicating any threats that might exist; and the future steps required for restoring systems and services. The Resolution Action Plan should be reviewed throughout the process as it may change depending on what evidence is required during the detection and analysis steps.

The key elements of the Resolution Action Plan are:

- **Containment actions** – what are you doing now to contain the incident/threat and prevent the spread of the situation?
- **Eradication actions** – what are you doing to remove the incident/threat from your environment?
- **Capability and capacity requirements** – what messages are you communication, to whom, and how?

The details of the Resolution Action Plan will vary depending on the type of incident that you experience.

5.2.2 Evidence Preservation

The IMT (or delegate) will collect and record evidence about the cyber incident to support detailed forensic investigations, including law enforcement efforts to identify and prosecute potential cyber-attacks.

To the best of its ability, and where relevant to the incident, the IMT (or delegate) should collect and record the following evidence:

- Hard drive images and raw images
- RAM images
- IP addresses
- Network packet capture and flows
- Network diagrams
- Log and configuration files
- Databases
- IR/investigation notes
- Screenshots
- Social media posts
- CCTV, video and audio recordings
- Documents detailing the monetary cost of remediation or loss of business activity

5.3 Communication and Engagement



5.3.1 Internal Communications

Beyond the regular situation reports, it may be necessary to brief all OTECH employees about a cyber incident. This is important, especially if the situation has potential to generate media or public interest.

All internal communications must be reviewed and approved by the OTECH CTO prior to release.

5.3.2 External Communications

Depending on the impact and severity of a cyber incident, it may be necessary to communicate with external stakeholders (including media and the public).

OTECH will work with Government of Guam Line Agencies and contractors to ensure that they identify and report all suspected or actual security breaches, incidents, and violations, including unauthorized or impermissible uses or disclosures comply with the policy described in this document. Security concerns, security incidents, or suspected/confirmed vulnerabilities will be shared with appropriate personnel in the organization so that the vulnerability can be remediated (or mitigated with compensating security controls) and we can ensure that similar vulnerabilities in other systems or processes can be addressed.

All external communications must be reviewed and approved by the OTECH CTO prior to release.

5.4 Recover

A Recovery Plan should be developed to detail the approach to recovering IT networks, systems and applications once containment and eradication is complete. The recovery plan should include the following elements:

- A plan to restore systems to normal operations
- A process of continual monitoring to confirm that the affected systems are functioning normally
- A plan (if applicable) to remediate vulnerabilities to prevent similar incidents.

5.4.1 Stand Down

Following the implementation and execution of an agreed recovery plan, the OTECH CTO should advise the IMT that it is acceptable to stand down.

5.5 Learn and Improve

This IMT and SEMT should come together for a Post Incident Review to discuss:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What should the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?



5.6 Update Incident Response Policy and Procedures

This plan will be continually updated to reflect better practice in cyber incident response activities, including following any relevant post incident reviews.

6.0 Compliance

Compliance with the policy defined in this document is mandatory. Failure to comply with OTECH Cyber Incident Response Policy may result in disciplinary actions up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. Failure to comply with OTECH Incident Response Policy may result in termination of contracts for contractors. Legal actions may also be taken for violations of applicable regulations and laws.